Remarks:

STATUS OF CLAIMS

Claims 1-20 are currently pending in the present application. Claims 13-20 are new and claims 1, 7, and 13 are independent.

Office Action

In the June 30, 2004, Office Action, the Examiner rejected claims 1-12. Specifically, the Examiner rejected claims 1-4 and 7-10 under 35 U.S.C. 102(b) as being anticipated by Russell (U.S. Patent No. 5,455,953) and rejected claims 5-6 and 11-12 under 35 U.S.C. 103(a) as being unpatentable over Russell in view of Hartman (U.S. Patent No. 5,960,411). Applicant respectfully suggests that the Examiner's cited references and all other prior art of record, alone or in combination, fail to disclose or suggest all claimed features of the present invention, namely storing authentication information on a user's computer, providing an authorization server with dynamic tracking abilities, utilizing an authorization server for purposes other than authentication, and allowing user or third-party access of data stored on the authorization server.

The present invention enables a user to log into an authorization server such that every application and server accessed by the user may authenticate the user without requiring a separate login for each server or application. Upon logging in, the authorization server creates a unique session ID for the user and stores data representative of at least a portion of the session ID on the user's computer. For example, if the user is utilizing a web browser, the authorization server may store a cookie on the user's computer including data representing the session ID. In addition to creating a session ID, the authorization server creates an object corresponding to the unique session ID and preferably stores the object on the authorization server. For example, the authorization server may create a computer-readable file corresponding to the session ID, place dynamic information regarding the session within the file, and then store the file in a directory accessible or otherwise coupled with the authorization server. After creating the object, the user may execute applications or access servers which may authenticate the user and modify the object by accessing the data stored on the user's computer, which represents the session ID, and then providing the session ID to the authorization server. Thus, a user is not required to specifically identify and

log-in to each accessed server or application. In contrast, the Examiner's cited references fail to disclose these features, as described below.

I. Russell fails to disclose or suggest storing authentication information on a user's computer

The portions of Russell cited by the Examiner (column 5, lines 35-55) for the basis that a session ID (SSDS 26) is stored on a user's computer are not relevant to the present invention as Russell's session ID, SSDS 26, is not utilized for authentication, but instead only provides connection compatibility between a client and various specified servers, which is the primary goal of Russell. As clearly stated by Russell, "the client, connection and session data structures thereby allow a Client 16 to operate in terms of requests, calls, or commands for operations to be performed for specified servers" (column 5, lines 54-58). Russell only stores authentication information on the authorization server 216 and accompanying directory server 218, neither of which reside within or otherwise coupled with a user's computer (column 21, lines 64-68). Applicant respectfully submits that the Examiner may not use Russell's disclosure of a session ID in a context completely unrelated to the present invention as a basis for rejection without showing that Russell *actually or implicitly* discloses or suggests the claimed functionality of the present invention. Applicant submits such a showing is impossible as Russell does not disclose or suggest storing authentication information on a user's computer.

As a result of failing to store authentication information on a user's computer, Russell requires user identification of a server each time the user desires to connect to the server. Specifically, "when user wishes to request an operation with respect to a Server 18, User will identify the Server to the LIA 220" (column 22, lines 32-40). The user is required to identify each server because Russell provides no other method or means for a server to determine how to authenticate a user. For example, if a user of Russell accesses a third party server (such as a web site with no affiliation to the user or authorization server), the third party server would have no means of determining how to authenticate the user, such as which authorization server or session ID to access as no authentication information is stored within the user computer or the third-party computer. Thus, if a user of Russell desires to access

9

many servers, the user is required to identify each server which may be cumbersome, difficult, or impossible due to the number and type of accessed servers.

In contrast, the present invention stores information relating to a session ID on a user's computer (such as within a browser-enabled cookie) such that **all** servers accessed by the user may utilize the stored information (the cookie) to automatically authenticate the user through the authorization server without requiring the user to consciously participate in the process. For instance, if a user of the present invention accesses a third-party server, the third-party server may receive the user's session ID by receiving a cookie stored on the user's computer and authenticate the user by providing the session ID to the authorization server. Thus, Russell fails to disclose storing data representative of at least a portion of the session ID on the user's computer, as required by all independent claims of the present invention.

II. Russell fails to disclose or suggest an authorization server having dynamic data

Russell's authorization server, and its accompanying directory server, only include static user information. Specifically, the user information of Russell does not change during any particular session, is not accessible or modifiable by a user (column 23, lines 10-20), and includes only static information such as a user display name or administrative information (columns 24, lines 60-67). The Examiner's rationale for concluding that Russell discloses "dynamic" session information is that Russell discloses "a Server that is involved in the session tracks the number of explicit and implicit calls or requests (Column 4 lines 64 - Column 13 line 10)." However, Russell's calls or requests are not stored or otherwise coupled with the authorization server or with other authentication information, and instead are stored entirely within the session control blocks, including SSB 32 and SSDS 26, which are entirely unrelated to authentication (column 12, lines 62-67), as discussed above. Thus, the "dynamic" information referenced by the Examiner is **not** dynamically stored in a directory coupled with the authorization server, as required by independent claims 1 and 7.

Similarly, Russell's tracking of explicit and implicit calls my not be utilized for authenticating and authorizing a user, as the stored explicit and implicit calls of Russell are not even accessible by the authorization server and are instead recorded only to "determine when the corresponding session 34 has no further outstanding calls 42 and may be deleted" (column 13, lines 7-10). When the session 34 has expired due a lack of

10

outstanding calls 42 is not utilized with or even relevant to authenticating user access. Thus, Russell completely lacks any disclosure or suggestion of *"dynamically* tracking a user session in order to authenticate and authorize a computer user."

III. Russell fails to disclose or suggest utilizing authentication information after a user is authenticated

Russell's disclosed authorization server and accompanying directory server are limited to performing the singular task of authenticating a user's access of a particular server operation (column 21 lines 48 - column 23 line 29). The Examiner has repeatedly cited Russell's SSDS 26 as disclosing many of the claimed features of the present invention. As discussed above in detail, the SDS 26 and SDS 32 of Russell are entirely unrelated to authentication and are utilized exclusively for connectivity comparability of a user computer. As a result, Russell does not disclose or suggest utilizing the authorization server or accompanying directory server for additional purposes, such as storing session information. Thus, a server which has received authentication information from the authorization server never accesses the authorization server for other purposes. In fact, Russell explicitly teaches away from having a server access an authorization server for purposes other than authentication, such as updating a shopping cart, as Russell seeks to minimize *server-authorization server* contacts (column 24, lines 25-52).

In contrast, the present invention seeks to minimize *user-server* contacts such that burdens on the user are minimized by allowing an authorization server to perform functions in addition to authentications, such as dynamically tracking the status of the user's session. For example, a user may execute an application, such as a java applet stored on a third-party web site, which authenticates the user. After authentication, the java applet may access and the authentication information to reflect a change in the session, as described below in detail. Russell fails to disclose or suggest this feature.

IV. Russell explicitly prevents user and third-party modification of authentication-server information

Russell's authorization server, as described by the Examiner, has access to various static authentication information, such as a user's name, access rights, and display

name (column 23, lines 1-5). Although this information is static information, and not dynamic information, as discussed above, all authentication information or data disclosed by Russell is not accessible or modifiable by a user because the information is encrypted with a server password (column 23, lines 10-15). Any entity which lacks the server password, such as a user or a third-party web-site, is unable to access or modify the data stored in the authorization server or directory server. Thus, the data stored within the authorization server may not be modified by a third party. For example, if a user attempts to place an item in a shopping cart on a third-party site, the third-party site and the user would be unable to modify data stored within the authorization server to indicate that the user had placed the item in the shopping cart because the user or third-party site do not have the server password.

In contrast, an object of the present invention is to enable various third-party servers to authenticate a user utilizing an authorization server and also allow the various third-party servers to modify session data associated with or included within authentication data. Such access and modification of session data allows the third-party servers to "modify the information in the object so that the object could pass information to other applications such as in a shopping cart environment" (page 7, lines 7-15). Russell teaches away from this concept as Russell's authorization server does not allow user or third-party access of data (column 23, lines 10-18).

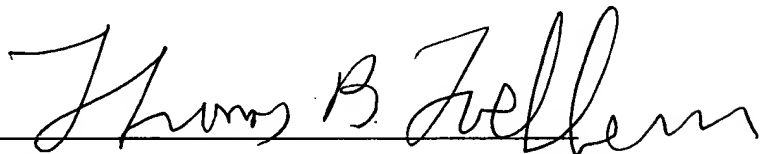### V. Hartman fails to correct the inadequate disclosure of Russell

The Examiner has stated that "Hartman discloses a method to include a shopping cart (FIG. 1A) and storing the shopping cart along with the object in the directory" (Office Action, page 10). In a previous Amendment, dated April 13, 2004, applicant argued that Hartman does not disclose any method used to track session information as Hartman merely discloses basic shopping cart-functionality. Thus, Hartman fails to correct the inadequate disclosures of Russell as Harman does not disclose any of the claimed features described in detail above, such as storing authentication information on a user's computer, providing an authorization server with dynamic tracking abilities, utilizing an authorization server for purposes other than authentication, or allowing user or third-party access of data stored on the authorization server.

12

VI. Conclusion

The Examiner's cited references, Russell or Hartman, fail to disclose or suggest all claimed features of the present invention such as storing authentication information on a user's computer, providing an authorization server with dynamic tracking abilities, utilizing an authorization server for purposes other than authentication, or allowing user or third-party access of data stored on the authorization server. Instead, the Examiner's references, including Russell, only disclose an authorization server having static information, which may not be modified or accessed by a user or third-party, and authentication information which is stored entirely on an authorization server such that user identification of a server is required each time the user desires to connect to the server.

In view of the remarks herein, applicant respectfully submits that claims 1-20 are in a condition for allowance. In the event of any questions, the Examiner is urged to call the undersigned. Any additional fee which might be due in connection with this application should be applied against Deposit Account No. 19-0522.

Respectfully Submitted,
HOVEY WILLIAMS LLP

By _____

Thomas B. Luebbering, Reg. No. 37,874
2405 Grand Boulevard - Suite 400
Kansas City, Missouri 64108
(816) 474-9050

(Docket No. 30604)

13